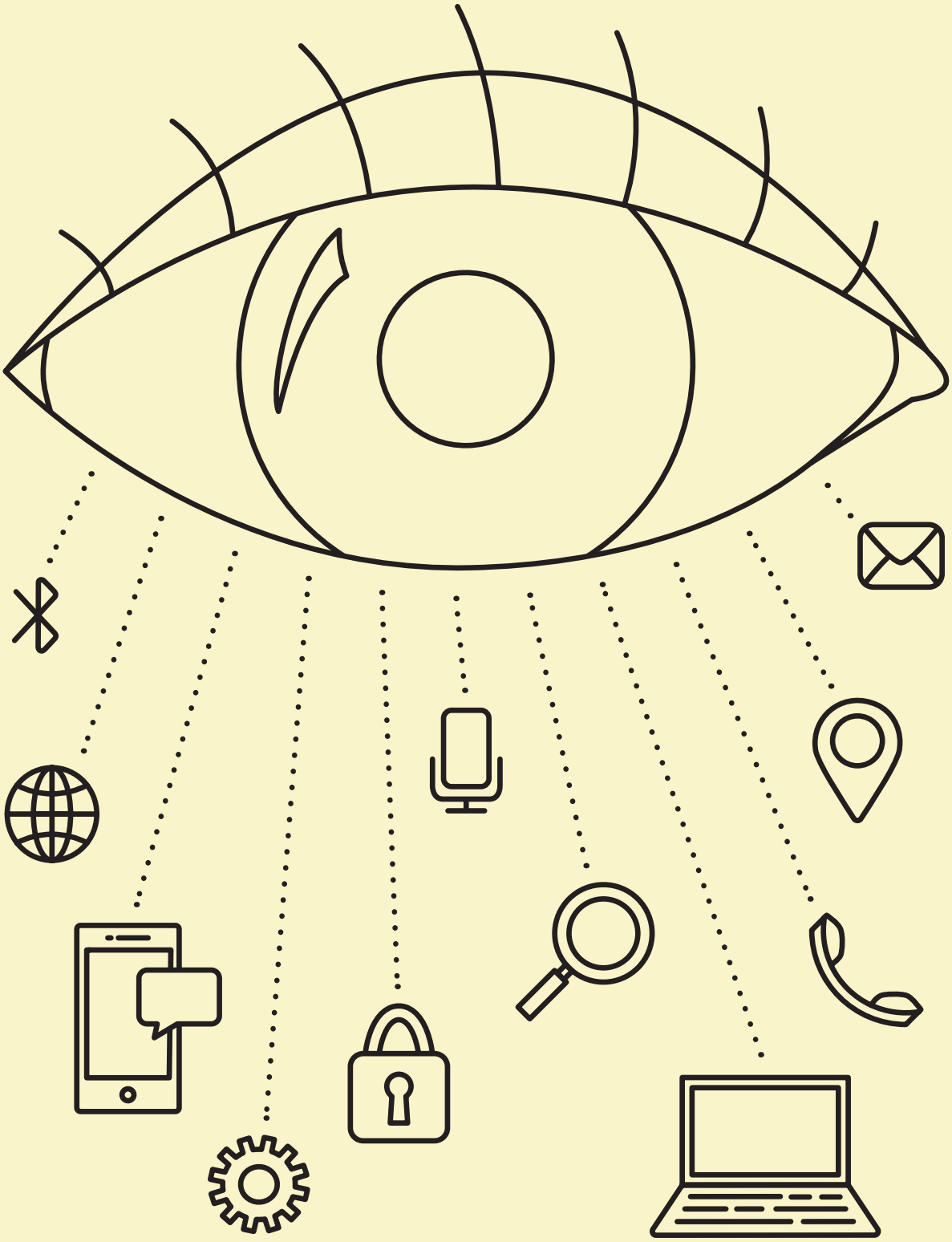

Was tun bei Technik- und Cyber-Stalking?

Handout

Stadt Wien

Kathrin Gaál
Vizebürgermeisterin und Stadträtin für Wohnen, Wohnbau, Stadterneuerung und Frauen. © David Bohman

Vorwort

Liebe Wienerinnen!

Unser Leben und unsere Kommunikation verlagern sich immer mehr ins Internet. Ein Alltag ohne Smartphone, PC oder Notebook/Tablet ist kaum noch vorstellbar. Digitale Kommunikation wird für uns alle, für jede Einzelne und jeden Einzelnen, immer wichtiger. Das bringt Vorteile, hat aber auch Schattenseiten.

Immer häufiger geraten Situationen online außer Kontrolle, und Frauen werden mit Cyber-Gewalt konfrontiert. Darunter fallen Cyber-Mobbing, Cyber-Stalking oder „Hass im Netz". Die zunehmende Digitalisierung hat leider auch bei Gewalt gegen Frauen in Beziehungen nicht haltgemacht.

Das vorliegende Handout „Was tun bei Technik- und Cyber-Stalking?" bietet eine Übersicht über wichtige Handlungsmöglichkeiten, wenn Stalking – also beharrliche Verfolgung – (zusätzlich) durch Nutzung technischer Möglichkeiten erfolgt.

Gleichzeitig kann das Handout nicht immer eine persönliche Beratung ersetzen. Oft braucht es eine Betrachtung der Gesamtsituation, um passende Handlungsstrategien zu erarbeiten und Sicherheitsstrategien zu planen. Die Beraterinnen des 24-Stunden Frauennotrufs und anderer Frauenhilfseinrichtungen, wie etwa der Wiener Frauenhäuser, unterstützen Sie dabei!

Denn jede Frau in Wien soll sicher, unabhängig und gewaltfrei leben können. Offline und online.

Kathrin Gaál
Wiener Vizebürgermeisterin und Frauenstadträtin

IMPRESSUM
Was tun bei Technik- und Cyber-Stalking?
Handout

Herausgeberin und Eigentümerin
Stadt Wien, Magistratsabteilung 57
Frauenservice der Stadt Wien
Kooperationsprojekt
Stadt Wien, Magistratsabteilung 57
Frauenservice der Stadt Wien und Saferinternet.at
Österreichisches Institut für angewandte Telekommunikation (ÖIAT)
Projektleitung Alina Zachar

Autorinnen Alina Zachar, Susanne Nagel, Barbara Buchegger
Lektorat Antonia Barboric
Illustrationen und Layout Jessica Gaspar

GENDERSENSIBLE SPRACHE
Da die Inhalte des Leitfadens auf Fallbesprechungen und Beratungen in Frauenberatungsstellen und Frauenhäusern basieren, wird in Verweisen von Tätern, Stalkern, Gefährdern sowie Klientinnen und Beraterinnen gesprochen.

1. Was tun bei Technik- und Cyber-Stalking?

Computer und besonders Handys können bei Gewaltbetroffenheit lebensrettend sein und wertvolle Informationen bieten. Gleichzeitig können sie jedoch auch missbräuchlich verwendet werden, z.B. zur Überwachung oder zur Verfolgung (Stalking). Nachstehend finden Sie Empfehlungen für die Sicherheitsplanung.

Vertrauen Sie Ihren Wahrnehmungen

Wenn Sie das Gefühl haben, dass der Gefährder „zu viel weiß", ist es möglich, dass er Ihr Telefon, Ihren Computer, E-Mail Account, Ihre Autofahrten oder andere Aktivitäten überwacht. Stalker können auf unglaublich hartnäckige und kreative Weise versuchen, Macht und Kontrolle zu erhalten – dadurch outen sie allerdings zugleich indirekt ihre Stalking-Methoden meist selbst.

Lassen Sie sich in einer spezialisierten Einrichtung (s. S. 6) beraten

- Nehmen Sie gemeinsam mit einer Beraterin eine Gefährdungs- und Risikoeinschätzung vor. Auf diese Weise wird Ihre Gesamtsituation erfasst, nicht nur das Technik-/Cyber-Stalking.
- Achtung bei Verhaltensänderungen: Diese können zu einer Erhöhung der Gefährdung oder Verlagerung der Stalking-Methode führen. Lassen Sie sich beraten.
- Notwendig sind außerdem eine gemeinsame Sicherheitsplanung, Informationen zur Beweismittelsicherung und das Aufzeigen Ihrer technischen und rechtlichen Möglichkeiten (z.B. Anzeige).
- Besondere Vorsicht ist geboten, wenn der Gefährder im IT-Bereich arbeitet oder spezielle Technikinteressen aufweist.

Zu beachten bei jeder Form des Stalkings

- **Fordern Sie zum Kontaktstopp auf, einmalig, unmissverständlich, schriftlich:** „Ich möchte in Zukunft auf keine Weise von dir kontaktiert werden." **Dokumentieren Sie die Aufforderung** zum Kontaktstopp.
- Antworten Sie nicht mehr.
- Blockieren Sie ggf. den Belästiger oder/und:
- Dokumentieren Sie jede weitere Form des Stalkings:
  - **immer** im Original (bei E-Mails, SMS, Sprachbox etc.)
  - zusätzlich mit Screenshots oder Sicherung der Aufzeichnungen
  - im Stalking-Tagebuch (alle anderen Kontaktaufnahmen)

Lassen Sie sich über die für Sie am wenigsten belastende Form der Beweismittelsicherung beraten.

Informationen zur Computer- und Online-Sicherheit

1. VERWENDEN SIE EINEN SICHEREREN COMPUTER
Insbesondere wenn der Täter Zugang zu Ihrem Computer hat oder hatte, ist es möglich, dass er Ihre Computeraktivitäten nun beobachtet. Achten Sie darauf, einen sichereren Computer zu verwenden, wenn Sie nach Hilfe, einer neuen Wohnung etc. suchen. Das ist z.B. ein Computer in einer Bibliothek, im Gemeindezentrum, in einem Internetcafé etc.

2. ERSTELLEN SIE EINEN NEUEN E-MAIL ACCOUNT, UND BEHALTEN SIE AUCH IHREN ALTEN E-MAIL-ACCOUNT
Wenn Sie vermuten, dass der Täter Zugriff auf Ihre E-Mails hat, erwägen Sie, auf einem anderen, sichereren Computer einen neuen E-Mail Account zu erstellen. Erstellen oder checken Sie diesen nicht von einem Gerät (Computer, Tablet oder Smartphone), auf das der Gefährder Zugriff hat oder hatte. Geeignet sind kostenlose E-Mail Accounts. Verwenden Sie zudem einen nicht identifizierbaren Namen und keine Länderinformation (z.B. yellowcat@gmail.com, nicht IhrRichtigerName@gmx.at).

3. ÄNDERN SIE ALLE PASSWÖRTER & PIN-CODES VON EINEM „SICHEREN" COMPUTER
- Denken Sie an alle von Passwörtern geschützten Accounts: Online-Banking, Amazon-Konten, FinanzOnline, WhatsApp, Clouds, WLAN, smarte Lautsprecher etc.
- Speichern sie keine Passwörter online, z.B. auf Webbrowsern.
- Melden Sie sich immer ab, wenn Sie die Anwendung nicht mehr brauchen.

Tipp für sichere Passwörter
Der Trend geht mittlerweile zu langen Passwörtern: Überlegen Sie sich einen (absurden) Satz mit einer Zahl, z.B.: „Morgens trinke ich immer 20 Semmeln." Verwenden Sie diesen Satz als Passwort. Ist die Zeichenanzahl vom Passwort beschränkt, verwenden Sie jeweils die Anfangsbuchstaben der einzelnen Wörter sowie die Zahlen und Satzzeichen von einem absurden Satz. Dies ist komplexer als das eigene Geburtsdatum und das der Kinder oder der Haustiername und trotzdem leicht merkbar.

4. COMPUTER NEU AUFSETZEN?

Haben Sie sich vom Gefährder getrennt, alle Passwörter geändert (inkl. WLAN), aber noch immer das Gefühl oder Hinweise vorliegen, dass der Computer überwacht wird?

- Probieren Sie, die Festplatte zu formatieren und den Computer neu aufzusetzen (nicht über die Backup-Version, sondern alle Programme wieder einzeln installieren).
- Achtung: Beim Formatieren der Festplatte gehen alle Einstellungen und Dokumente, Fotos etc. verloren.
- Falls Sie Sicherungskopien erneut auf den Computer laden, laufen Sie Gefahr, unbeabsichtigt ebenso wieder Software zu installieren, die Ihren Computer unsicher macht.

Lassen Sie sich über verschiedene Möglichkeiten, den Computer sicher wieder aufzusetzen, und weitere Aspekte der Sicherheitsplanung beraten.

5. FACEBOOK UND ANDERE SOZIALE MEDIEN

Überprüfen Sie, auch gemeinsam mit Ihren Kindern, regelmäßig die Privatsphäre-Einstellungen von Facebook und sonstigen sozialen Netzwerken. Wägen Sie zuvor ab, wie wichtig es für Sie ist, diese Netzwerke zu nutzen.

- Auf der Website von Safer Internet sind aktuelle Leitfäden zu Privatsphäre-Einstellungen erhältlich: **saferinternet.at/privatsphaere-leitfaeden**
- Allgemeine Empfehlungen bei allen sozialen Medien:
  - **Sichern Sie Beweise im Original und/oder mittels Screenshots oder Netzbeweis.com** (= ein z.T. kostenloses Programm mit dessen Hilfe ein Screenshot mit den notwendigen Metadaten abgespeichert werden kann).
  - Blockieren Sie den Belästiger (lassen Sie sich beraten, ob diese Empfehlung für Ihre Situation passend ist).
  - **Melden Sie Beiträge** bei der jeweiligen Plattform (s. Punkt 6).
  - **Stellen Sie Ihre Konten auf „privat".**
  - Lassen Sie in Profilbildern und auf Fotos keine Rückschlüsse auf Personen zu.
  - im Nickname keine Rückschlüsse auf Alter, Geschlecht und Wohnort zulassen
  - Deaktivieren Sie die „Sichtbarkeit" (ob Sie gerade online sind).
  - **Durchforsten Sie Ihre „Gruppen",** ob der Belästiger Teil einer Gruppe ist.

6. FAKE ACCOUNTS UND BELÄSTIGENDE BEITRÄGE IN SOZIALEN MEDIEN MELDEN

- **Sichern Sie Beweise im Original, z.B. mithilfe von Screenshots (v.a. bei verschwindenden Nachrichten) und/oder mit Netzbeweis.com.** Datum und soziale Plattform im Stalking-Tagebuch dokumentieren.
- **Melden Sie Beiträge:** In allen sozialen Netzwerken gibt es die Möglichkeit, Fake Accounts oder Beiträge zu melden. Bei den meisten sozialen Netzwerken ist es gleich bei jedem Beitrag möglich, diesen zu melden.
- Rechtswidrige Inhalte (z.B. § 105, § 107, § 107a, § 107c, § 113, § 120, § 144, § 207, § 208a) sind im Rahmen des **Hass-im-Netz-Bekämpfungs-Gesetzes (HiNBG)** und des **Kommunikationsplattformen-Gesetzes (KoPl-G)** von größeren Kommunikationsplattformen innerhalb von 24 Stunden nach deren Meldung zu löschen. Es muss explizit angegeben/angeklickt werden, dass Inhalte gemäß KoPl-G rechtswidrig sind.
- Falls der Beitrag nicht gelöscht wird, können Sie sich an die RTR – Rundfunk und Telekom Regulierungs-GmbH wenden und Beschwerde einreichen (Kontakt s. S. 6).

Weitere Unterstützungsmöglichkeiten, wenn Fake Accounts oder Beiträge trotz Meldung nicht (schnell genug) gelöscht wurden:

- **Beratungsstelle ZARA – gegen** alle Formen von **Hass im Netz**
- **Ombudsstelle.at:** Meldung an die Internet-Ombudsstelle vor allem für Facebook, Instagram, YouTube, Twitter, Snapchat. Auf der Website sind auch allgemeine Informationen zu Internetsicherheit, Bildrechten etc. zu finden.

Sowohl ZARA als auch die Internet-Ombudsstelle sind Trusted Flag User. D.h., bedrohliche Inhalte aus sozialen Medien können (meist) schneller gelöscht werden.

- Lassen Sie sich beraten, ob ein **Mandatsverfahren** (Antrag auf Erlassung eines Unterlassungsauftrags) möglich und sinnvoll ist (Achtung auf mögliche Kosten).

7. SUCHEN SIE IHREN NAMEN IM INTERNET

Große Suchmaschinen wie Yahoo, Google etc. können möglicherweise Kontaktinformationen enthalten. Geben Sie bei der Suche Ihren Namen unter Anführungszeichen – „Ihr Name" – ein. Durchsuchen Sie Telefonbücher und Verzeichnisse. Bei Falschinformation über Ihre Person im Internet kontaktieren Sie den*die Betreiber*in der Seite bzw. lassen Sie sich über weitere Möglichkeiten beraten.

8. NUTZEN SIE DAS „RECHT AUF VERGESSEN" BEI SUCHMASCHINEN WIE GOOGLE, BING:

Beim „Recht auf Vergessen" handelt sich lediglich um ein „Vergessen" von Verlinkungen. Die Inhalte sind nach wie vor vorhanden, aber über eine Internetsuche (in europäischen Ländern) nicht mehr auffindbar. Trotzdem ist dies eine empfehlenswerte Möglichkeit, v.a. wenn ein Stalker viele (Falsch-)Informationen ins Netz gestellt hat. Die Inhalte müssen dann im Netz mit etwas mehr Aufwand recherchiert werden.

Formular:
- support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de
- bing.com/webmaster/tools/eu-privacy-request

Information zu Smartphone- und Handysicherheit:

9. ÜBERPRÜFEN SIE IHRE HANDY-EINSTELLUNGEN, VOR ALLEM WENN DER STALKER DIREKTEN ZUGRIFF AUF IHR HANDY HATTE
- Schalten Sie das Handy bei wichtigen/vertraulichen persönlichen Gesprächen aus.
- Achten Sie, dass die Sicherheitseinstellungen auf Ihrem Handy aktiviert sind (z.B. Google Play Protect).
- Deaktivieren Sie alle GPS-Funktionen (auch auf dem Computer).
- Ändern Sie alle Passwörter, die Tastensperre und PINs.
- Achten Sie besonders auf Schnittstellen wie Backups oder vom Computer aus steuerbare Apps (z.B. „Find my phone", Messenger-Dienste etc.).
- Allerdings: Selbst bei ausgeschalteter GPS-Funktion kann eine ungefähre Lokalisierung über Handymasten erfolgen. Ebenso werden im eingeschalteten Flugzeugmodus GPS-Daten gesendet.

10. HANDY AUF WERKSEINSTELLUNGEN ZURÜCKSETZEN?
Sichern Sie zuerst die Ihnen wichtigen Daten, Fotos und Musik. Alle persönlichen Einstellungen und Apps, aber auch die Einstellungen des Stalkers gehen verloren, wenn das Smartphone auf Werkseinstellungen zurückgesetzt wird. Installieren Sie keine Programme oder Anwendungen über das Backup des Computers. Alle Apps und Anwendungen sind einzeln neu zu installieren. Lassen Sie sich über die einzelnen im Detail für die Sicherheitsplanung zu beachtenden Arbeitsschritte beraten.

11. VERWENDEN SIE EIN NEUES HANDY – UND BEHALTEN SIE IHR ALTES HANDY/SMARTPHONE
- Lassen Sie Ihre Nummer mit dem neuen Handy nicht in einem Telefonverzeichnis eintragen, wählen Sie eine Geheimnummer.
- Als neues Handy eignen sich zunächst insbesondere alte, noch funktionsfähige Handys (keine Smartphones), da diese über weniger Funktionen verfügen.
- Behalten Sie das Handy mit der alten Nummer, und verwahren Sie es an einem sicheren Ort, z.B. Abstellraum.

12. ACHTUNG: BEI SMS WIRD IMMER DIE NUMMER MITGESCHICKT
Wenn Sie ihre Handynummer auf „unbekannt" stellen und ein SMS schreiben, wird trotzdem Ihre Handynummer mitgesendet!

13. BEWEISMITTEL SAMMELN – HANDY
Wenn es für Sie möglich ist, behalten Sie auch Ihre alte Handynummer. Wenn der Stalker auf die Mailbox spricht und SMS schreibt, antworten Sie nicht! Eine Nachricht seinerseits dient allerdings als Beweis für eine Kontaktaufnahme und Bedrohung. Speichern Sie die Beweise, und kontaktieren Sie die Polizei.

14. SPEICHERN SIE BEWEISE IMMER IM ORIGINAL
Speichern Sie alle Beweise von elektronischen Kontaktaufnahmen immer im Original. Im Original bleiben Metadaten (= Hintergrundinformationen) vorhanden. Lassen Sie sich über die für Sie am wenigsten belastende Form der Beweismittelsicherung beraten.

15. „INTERNET OF THINGS" (IOT) – „SMARTE" GERÄTE
„Internet of Things" (IoT) oder auf Deutsch „Internet der Dinge" beschreibt Technologien, die es ermöglichen, dass sich reale und virtuelle Dinge miteinander vernetzen. Dazu zählen „smarte" Geräte, smarte Lautsprecher, smarte Fernseher, smarte Heizungssysteme etc.
- Bringen Sie in Erfahrung, was Ihre „smarten" Geräte tatsächlich alles können und was sie nicht können.
- Vorsicht bei smarten Lautsprechern, die über Sprachbefehle steuerbar sind, vor allem wenn der Belästiger Zugang zu den Geräten hatte.
- Stellen Sie sicher, dass Sie die Zugangsdaten und Passwörter von allen smarten Geräten in Ihrem Haushalt haben. Ändern Sie, wenn notwendig, Passwörter und Zugangsdaten.
- Überprüfen Sie, mit welchen anderen smarten Geräten Verknüpfungen bestehen, und ob Sie diese Geräte kennen.
- Zu erwägen ist auch die Frage, ob alle sogenannten Unterstützungstechnologien überhaupt gebraucht werden.

Weitere Information zur Wahrung Ihrer Privatsphäre:

16. ACHTEN SIE AUF IHRE DATEN, DIE SIE BEI BONUSKARTEN UND DERGLEICHEN (Z.B. BEI SUPERMÄRKTEN) ANGEGEBEN HABEN
Über Ihren richtigen Namen kann sehr leicht Ihre neue Adresse eruiert werden.

17. VERLANGEN SIE IHRE DATEN UND AKTEN
Fragen Sie Institutionen, wie diese Ihre Daten schützen oder veröffentlichen, und erlauben Sie nur den geringstmöglichen Zugang zu Ihren Daten (Gericht, Spital, Ärzt*innen etc.).

18. MIETEN SIE EIN POSTFACH
Geben Sie die Postfachadresse bei Geschäften, Ärzt*innen und anderen wichtigen Stellen an. Überlegen Sie eine Auskunftssperre beim Melderegister. Versuchen Sie zu verhindern, dass Ihre richtige Adresse in Telefonbüchern und Datenbanken gelistet wird.

2. Nützliche Links

Beratungseinrichtungen und Information zu Technik- und Cyber-Gewalt in Beziehungen

24-Stunden Frauennotruf der Stadt Wien
› Telefon: 01 71 71 9
› Web: frauennotruf.wien.gv.at

Ergänzendes Beratungsangebot durch die Kompetenzstelle gegen Cyber-Gewalt:
Im Rahmen der Kompetenzstelle gegen Cyber-Gewalt der Stadt Wien können die IT Sicherheitsexpert*innen der Stadt Wien (WienCERT) von den Beraterinnen des 24-Stunden Frauennotrufs bei Bedarf bei technischen Fragen beigezogen werden.

Wiener Frauenhäuser

Beratungsstelle der Wiener Frauenhäuser:
› Telefon: 01 512 38 39

Gruppenangebot für Frauen zum Thema Cyber-Gewalt:
› Web: frauenhaeuser-wien.at/gruppenangebote.htm

Frauenhaus Notruf:
› Telefon: 05 77 22

Ergänzendes Beratungsangebot durch die Kompetenzstelle gegen Cyber-Gewalt:
Auch Beraterinnen der Wiener Frauenhäuser können im Rahmen der Kompetenzstelle gegen Cyber-Gewalt der Stadt Wien die IT-Sicherheitsexpert*innen der Stadt Wien (WienCERT) bei Bedarf bei technischen Fragen beiziehen.

Gewaltschutzzentrum Wien
› Telefon: 01 585 32 88
› Web: interventionsstelle-wien.at

Frauenhelpline gegen Männergewalt
› Telefon: 0800 222 555

Frauen* beraten Frauen*
› Telefon: 01 587 67 50

Online-Beratungsangebot:
› Web: frauenberatenfrauen.at

Landeskriminalamt Wien, Kriminalprävention
› Telefon: 0800 21 63 46
Meist Anrufbeantworter. Sie werden zurückgerufen.

ZARA Beratungsstelle bei (allen Formen von) Hass im Netz/Hatespeech
› Telefon: 01 929 13 99
› Web: zara.or.at/de/beratungsstellen/GegenHassimNetz

FairesNetz
› Web: fairesnetz.at

Internet-Ombudsstelle
› Web: ombudsstelle.at

Safer Internet
Keine persönliche Beratung.
Viele nützliche Informationen,
Leitfäden zu Internetsicherheit
› Web: saferinternet.at

Information und Hilfestellung für Opfer von Stalking
› Web: stalking.at

Netzbeweis.com
Unterstützung bei gerichtstauglicher Beweismittelsicherung in sozialen Medien
› Web: netzbeweis.com

RTR – Rundfunk und Telekom Regulierungs-GmbH
Einreichung von Beschwerden, wenn ein strafrechtlich relevanter Beitrag in (großen) sozialen Medien trotz Meldung (nach dem Kommunikationsplattformengesetz KoPl-G) nicht gelöscht wurde.
› Web: beschwerde.rtr.at/startseite.de.html